REMARKS

In response to the Office Action mailed September 22, 2005, Applicants respectfully request reconsideration. The pending claims are believed to be in allowable condition.

Claims 1-3, 6-12, 15-20 and 22-26 were pending in this Application. By this Amendment, claim 20 has been canceled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Accordingly, claims 1-3, 6-12, 15-19 and 22-26 are now pending in this Application. Claims 1, 10, 19 and 22 are independent claims.

Rejections under §102 and §103

Claim 20 was rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,816,968 (Walmsley). It is respectfully submitted that this rejection is no longer applicable due to the cancellation of claim 20.

Claims 1-3, 6-7, 20-12, 15-16, 19 and 22 were rejected under 35 U.S.C. §103(a) as being unpatentable over Walmsley in view of U.S. Patent No. 6,073,118 (Gormish). Also claims 1, 10 19 and 22 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walmsley in view of U.S. Patent No. 6,484,128 of Sekiya. Claims 23-26 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Walmsley in view of Gormish, the Handbook of Applied Cryptography (Menezes) and Sekiya. Applicants respectfully traverse each of these rejections and request reconsideration.

In order to establish a *prima facie* case of obviousness, the Office Action must meet three criteria.

> "First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations."

In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

It is respectfully urged that the claims rejections do not satisfy the above requirements, and that therefore the rejections should be withdrawn and the claims allowed.

Claim 1 recites a method for verifying that a module is from an approved vendor, which comprises (1) obtaining vendor data including a module serial number from a module, (2) obtaining a second serial number of a second module, and (3) outputting a serial number valid signal when the module serial number of the vendor data does not match the second serial number from the second module, and a serial number invalid signal when the serial number of the vendor data matches the second serial number from the second module. As described in the application, this method can be used to detect a module from a particular type of non-approved vendor, namely the non-approved vendor who simply copies the vendor data (including serial number) from an approved vendor. While the testing of the magic codes will succeed, which by itself would indicate that the module is from an approved vendor, the detection of a duplicate serial number will indicate that the module has copied vendor data and therefore may not be from an approved vendor.

Walmsley is concerned with the problem of authenticating so-called "consumables" such as printer ink cartridges and camera film. Walmsley teaches several authentication techniques in which one or two devices (such as devices 21 and 23 in Figure 3) exchange messages with a chip 20 in an object being authenticated. It is a fundamental assumption in Walmsley that the chip 20 includes one or more encryption keys that the chip uses to perform certain encryption/decryption tasks during the authentication process (col. 24 lines 46-48; col. 26 lines 46-49). Moreover, it is a further fundamental assumption that the secret keys are kept secret (col. 25 lines 13-14; col. 26 lines 2-5), and the chip's data storage integrity is secure (col. 25 lines 60-63). Thus, Walmsley is

not concerned with the problem that a clone manufacturer will directly copy an authentication chip. Indeed, the various attack scenarios described in section 5.5 of Walmsley (col. 29 lines 25 to col. 57 line 50) do not include any such direct copying, but rather different kinds of attempts to glean the keys by observing the behavior of the authentication chip in response to certain stimuli.

Thus, Walmsley has no need of any technique for comparing serial numbers from different consumables. Operating on the stated assumptions of key security and memory storage security, any of Walmsley's authentication processes is sufficient by itself to establish the authenticity of a given consumable. Comparing serial numbers or any other consumable-specific value would be redundant and unnecessary.

Gormish is concerned with the problem of ensuring security of financial transactions that are conducted by facsimile, and proposes a "label" that includes encoded customer-specific information. Each label may have a unique serial number that serves a security-related purpose. The serial number can be compared against a list of serial numbers of previous transactions that are kept at a "verifying location" for each transaction such as a bank or credit company. If a match is found, then the transaction can be rejected because of the apparent duplicate use of a label.

It will be appreciated that the label being authenticated or validated in Gormish is very different from the authentication chip in Walmsley. The entire contents of the label are easily read and reproduced. Moreover, the label is a passive item that cannot actively perform encryption and decryption, in contrast to the authentication chips of Walmsley. Where Walmsley relies on the secrecy of the keys and security of the memory of its authentication chip, the financial transaction processing system of Gormish has no similar capability. Gormish must protect a transaction that is identified only by a passive, completely visible piece of paper. Gormish does this by assigning serial numbers to the labels and detecting whether there is any duplicate use of a serial number. Gormish uses a technique of assigning and comparing serial numbers because of the specific

operating environment - a high volume of financial transactions that are identified using easily reproduced paper labels. Walmsley's operating environment is different - each consumable is identified by an active authentication chip having securely stored keys that cannot be reproduced (and indeed are not visible from outside the chip). Walmsley has no need of a serial number comparing technique such as that of Gormish because Walmsley already has other ways of addressing the problem of duplication - maintaining secrecy of the keys and ensuring the security of the memory storage within the authentication chip.

Moreover, it should be appreciated that if a manufacturer of clone consumables were to be able to completely duplicate an authentication chip (which duplication could be detected by comparing serial numbers of different authentication chips), it would mean that the clone manufacturer could duplicate the keys as well as the encryption/decryption algorithms. Once the clone manufacturer can duplicate these items, it need not duplicate any other data - it has the power to generate valid encryptions of arbitrary memory data including arbitrary serial numbers. In the face of that kind of cloning scenario, the printer manufacturer would have no reason to believe that it can detect clones by comparing serial numbers, because it could not be assumed that the clone manufacturer would use duplicate serial numbers (and in fact a smart clone manufacturer in this position would not). Thus there would be no reason to incorporate a duplicate-serial-number detection scheme such as that of Gormish into the Walmsley system - it would only add to the system's complexity without any guarantee of commensurate effectiveness. Thus, contrary to the suggestion in the Office Action, the use of Gormish's serial-number-comparing technique would not prevent unauthorized re-use of a print cartridge any more than Walmsley's authentication technique already does. If the assumptions of key security and memory storage security are satisfied, then any checking of serial numbers would be unnecessarily redundant. And if those assumptions are not satisfied, Walmsely's technique would have to be modified in some other more fundamental manner, because the clone-maker would not be constrained to use

duplicates of serial numbers or any other data and therefore could not be detected by detection of such duplicates.

Thus it is respectfully urged that Walmsley and Gormish do not include any motivation to combine their respective teachings, notwithstanding the contrary assertion in the Office Action. Accordingly, these references cannot render claim 1 obvious under 35 U.S.C. § 103(a).

Sekiya shows a data processing system having increased reliability through use of configuration management that tracks the failures and properties of different modules. Part of the configuration management includes information about the vendor and version number for each module. When the configuration management system detects the installation of a module whose version number indicates a potential compatibility problem, it provides a corresponding alert so that there is an opportunity to replace the module with one having greater compatibility.

The Office Action has equated the "serial numbers" of claim 1 with the "version numbers" of Sekiya, but this is inaccurate. A version number is not a serial number. A version number is only unique to a module "version", and not to an individual module. There may be hundreds or thousands of modules having the same version number. Any attempt to defeat clone manufacturers by using version numbers would be highly ineffective. The method of claim 1 requires the use of module serial numbers, which as known in the art are numbers that uniquely identify individual modules. The Examiner is referred to lines 4-10 of page 8 of the present application, for example, which describe this characteristic of the module serial numbers.

Thus even if Sekiya is combined with Walmsley as set forth in the Office Action, the result does not include any technique for comparing the serial numbers of different modules. Accordingly, the combination of Walmsley and Sekiya cannot render claim 1 obvious under 35 U.S.C. § 103(a).

Because all the remaining claims recite, either directly or indirectly, features such as those discussed above with respect to claim 1, the remaining

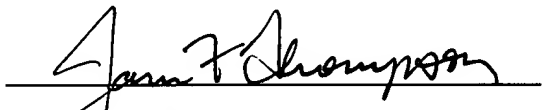
claims are also not rendered obvious by Walmsley in combination with either Gormish or Sekiya.

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If there should be any issues remaining after this Amendment, the Examiner is respectfully requested to call the Applicants' Representative at the number below if such issues can be resolved thereby.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned attorney.

Respectfully submitted,



James F. Thompson, Esq.
Attorney for Applicant(s)
USPTO Registration No.: 36,699
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road, Suite 2A
Westborough, MA 01581
Tel: (508) 616-2900
Fax: (508) 366-4688

Attorney Docket No.: CIS01-25(4997)

Dated: December 22, 2005